TOSTARY	(2005) (an	07/28/2005
AUG 0 1 2005	Under the Paperwork F	Reduction Act of 1995, no per

PTO/SB/08a (08-03) Approved for use through 07/31/2006. OMB 0651-0031

Approved for use directly 07/3 1/2000. Cities 0001-0001

AUG U 12	Index the Pagerwork Reduction Act of 1995, no persons are required to respond to a collection of info unless it contains a valid UMB control number.								
- Cubatitu	as form	n 1449A/PTO			Com	plete if Kn	own		
THE STATE OF THE S	101 10111	11111070110		Application Number 10/005,1		10/005,10	)5		
INFO	RMAT	ION DISCLOSURE		Filing Da		Decembe	r 3, 2001		
		T BY APPLICANT			ned Inventor	Paul C. K	ocher		
		•		Group Ar		2132			
	(use as	many sheets as necessa	ry)	Examine		Justin T.	Darrow		
Sheet	1	of 3		Attorney	Docket No.r	44424162	2-8721		
0.11001	Class /Sub class								
Examiner	Cite	Document Number		PATENT DOCUMENTS  ublication Date			Peges, Columns, Lines, Where Relevant Passages or		
Initials*	No.¹	Number-Kind Code <sup>2 (If known)</sup>		DD-YYYY		Docoment	Relevant Figures Appear		
M		4,211,919		/1980	Michel Ugon		234/407		
na_		4,295,041 A		/1981	Michel Ugon	<u></u>	307/206.5		
ŶΩ ΩΩ		4,916,333 A		/1990	Jacek Kowalsk		3,90/4		
JP_		4,932,053 A		/1990	Serge Fruhauf		3,40,47		
N -		5,297,201 🖯		2/1994	John H. Dunla		70/6		
80		5,412,723 A		2/1995	Ran Canetti et		3,00/2/		
10		5,636,157 A		3/1997	James H. Hess	on et al.	364/780		
m		5,991,415 A		3/1999	Adi Shamir		380/30		
ñn		6,434,238 B1	08/13	3/2002	David Chaum		340(4)		
30		6,698,662 B1	03/02	2/2004	Nathalie Feyt	et al.	235/492		
				<u> </u>					
	1		1		1		l		

Examiner Initials\*

Cite No.1 Foreign Patent Number Publication Date MM-DD-YYYY Publication Date MM-DD-YYYY Applicant of Cited Document Passages or Relevant Figures Appear

Examiner Signature Out Juny Date Considered 09/29/2005

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. Applicant's unque citation designation number (optional). See Kinds Codes of USPTO Patent Documents at <a href="https://www.uspto.gov">www.uspto.gov</a> or MPEP 901.04. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. Applicant is to place a check mark here if English tanguage Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to This collection of information. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete some submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete some submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete some submitting the completed application. Submitted the complete some submitting the complete some submitting the complete some submitted to take 2 hours to complete, including gathering, preparing, preparing, process) an application. Confidentially is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is required to obtain or retain a benefit by the public which is to file obtained by the USPTO to obtain or retain a benefit by the public which is to file obtained by the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete and submitted the process of the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete and submitted the process of the USPTO. The public variety of the USPTO

U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of info unless it contains a valid OMB control number.

Submits	ite for form 14491	R/PTO		Complete if Known		
Substitu	NC LOT TOTAL 14421	5,110		Application Number	10/005,105	
INFO	RMATION	DISCI	OSURE	Filing Date	December 3, 2001	
	TEMENT B			First Named Inventor	Paul C. Kocher	
				Group Art Unit	2132	
	luse as n	nanv sheet	s as necessary)	Examiner Name	Justin T. Darrow	
Sheet	2	of	3	Attorney Docket No.	44424162-8721	

		OTHER ITEMS – NON PATENT LITERATURE DOCUMENTS					
Examiner Initials*	Cite No.1	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T <sup>2</sup>				
		BACK, Adam, "Non-Interactive Forward Secrecy" 09/06/1996					
-W		BELL, Jim, "Spread-Spectrum Computer Clock?" Google Beta Groups					
AP		BELLARE et al., "Optimal Asymmetric Encryption", Advanced Networking Laboratories, 1998, pp 92-111, Springer-Verlag, U.S.A.					
<u></u>		BELLARE et al, "The Exact Security of Digital Signatures- How to Sign with RSA and Rabin", Advances in Cryptology - Eurocrypt 96 Proceedings, Lecture Notes in Computer Science, Vol. 1070, , pp 1-16, U. Maurer ed.,					
W	<u> </u>	Springer-Verlag, 1996  BELLARE et al, "Forward Integrity For Secure Audit Logs", pp 1-16,	$\vdash$				
AO	İ	November 23, 1997, U.S.A.	L				
ar Ar		FRANKEL et al., "Optimal-Resilience Proactive Public-Key Cryptosystems" IEEE Symposium on Foundations of Computer Science, 1997					
<del>gi</del> Q0		FRANKEL et al., "Proactive RSA", Lecture Notes in Computer Science, 1996					
10		HERZBERG et al, "Proactive Public Key and Signature Systems", ACM Conference on Computer and Communications Security, 1996					
Examin Signatu		Oustrin Borner Considered 09/29/2005					

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. ¹ Applicant's unque citation designation number (optional). ² See Kinds Codes of USPTO Patent Documents at <a href="https://www.uspto.gov">www.uspto.gov</a> or MPEP 901.04. ³ Enter Office that Issued the document, by the two-letter code (WIPO Standard ST.3). ¹ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁵ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁶ Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file ( and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Approved for use through 07/31/2006. OMB 0651-0031

U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of info unless it contains a valid OMB control number. Complete if Known form 1449B/PTO Substitute 10/005,105 **Application Number** December 3, 2001 INFORMATION DISCLOSURE Filing Date STATEMENT BY APPLICANT Paul C. Kocher First Named Inventor 2132 **Group Art Unit** Justin T. Darrow (use as many sheets as necessary) **Examiner Name** 44424162-8721 Attorney Docket No. of 3 Sheet OTHER ITEMS - NON PATENT LITERATURE DOCUMENTS Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the T<sup>2</sup> item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), Examiner Cite No. publisher, city and/or country where published. Initials\* MENZES et al, "Pseudorandom Bits and Sequences", Handbook of Applied Cryptography, CRC Press, Chapter 5, pp 169-190, 1996 MENZES et al, "Efficient Implementation", Handbook of Applied Cryptography, CRC Press, Chapter 14, pp 591-634, 1996 RIVEST, Ronald, "Timing Cryptanalysis of RSA, DH, DDS" Google Beta Groups Date Examiner 09/29/2005 Considered Signature

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. Applicant's unque citation designation number (optional). See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. <sup>3</sup> Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). <sup>4</sup> For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. Skind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. <sup>6</sup> Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file ( and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

## 10/005,105 **Application Number** INFORMATION DISCLOSURE December 3, 2001 Filing Date STATEMENT BY APPLICANT Paul C. Kocher **First Named Inventor** 2132 **Group Art Unit** Justin T. Darrow (use as many sheets as necessary) **Examiner Name** 44424162-8721 Sheet **Attorney Docket Number**

		U.	S. PATENT DO	CUMENTS	
Examiner Initials*	Cite No. <sup>1</sup>	Document Number Number-Kind Code <sup>2 (# known)</sup>	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Documen	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
			· · · · · · · · · · · · · · · · · · ·		
				•	
· • • • • • • • • • • • • • • • • • • •					
		FOF	REIGN PATENT D	OCUMENTS	C. 6 15/505(las)
Examiner Initials*	Cite No.1	Foreign Patent Number  Country Code <sup>3</sup> Number <sup>4</sup> Kind Code <sup>5</sup> (if kn	Publication Da		Pages Columns Lines, Where Relevant Passages or Relevant Figures Appear
m		EP 90201136.0 A1	11/28/199		H042 9/06

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. Applicant's unque citation designation number (optional). See Kinds Codes of USPTO Patent Documents at <a href="https://www.uspto.gov">www.uspto.gov</a> or MPEP 901.04. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

( OS ( OS / OS / 2005 ) ( OM O4/2P/2005

EP 0 656 708 A1

PTO/SB/08a (08-03)

Approved for use through 07/31/2006. OMB 0651-0031

404L 9/0P

U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

WWY A.	ote for form 1449A/I			Co	omplete if Known
0000				Application Number	10/005,105
INFO	DRMATION D	ISC	LOSURE	Filing Date	December 3, 2001
STATEMENT BY APPLICANT				First Named Inventor	Paul C. Kocher
				Group Art Unit	2132
	(use as many sl	heets	as necessary)	Examiner Name	Justin T. Darrow
Sheet	T1	of	2	Attorney Docket Number	44424162-8721

		U	J.S. PATENT DO	CUMENTS	(651/545class
Examiner Initials*	Cite No.1	Document Number  Number-Kind Code <sup>2 (If known)</sup>	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Rages, Columns, Lines Where Relevant Passages or Refevant Figures Appear
M		4,799,258 A	01-17-1989	Donald Davies	380/21
AO		5,506,905 A	04-09-1996	Dale Markowski et al.	380/20
(20)		5,546,463 A	08-13-1996	Anthony A. Caputo et al.	380/25
		FC	OREIGN PATENT D	DOCUMENTS	(6, 5, 5, 6, 6, 6, 1)
Examiner Initials*	Cite No.1	Foreign Patent Number  Country Code <sup>3</sup> Number Kind Code <sup>5</sup> (if k	Publication Da	ate Name of Patentee or	Pages, Columns, Lines Where Relevant Passages or Relevant Figures Appear

Examiner Signature	Mostin Danger	Date Considered	09/29/2000

06-07-1995

International
Business Machines

Corporation

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. ¹ Applicant's unque citation designation number (optional). ² See Kinds Codes of USPTO Patent Documents at <a href="https://www.uspto.gov">www.uspto.gov</a> or MPEP 901.04. ³ Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). ⁴ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁵ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁶ Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file ( and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Approved for use through 10/31/2002. OMB 0651-0031

U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Under the Paperwork 16 of 1995, no persons are required to respond to a collection of info unless it contains a valid OMB control no.

Please type a p

Substitu	te for form 1449B/PT	o		Complete if Known		
				Application Number	10/005,105	
	RMATION DI			Filing Date	December 3, 2001	
STAT	TEMENT BY	APP	LICANT	First Named Inventor	Paul C. Kocher	
				Group Art Unit	2132	
	(use as many	sheet	s as necessary)	Examiner Name	Justin T. Darrow	
Sheet	2	of	2	Attorney Docket Number	44424162-8721	

OTHER ITEMS – NON PATENT LITERATURE DOCUMENTS						
Examiner Initials*	Cite No.'	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T <sup>2</sup>			
00		KOCHER, P., "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems", 08/18/1996 XP000626590.				
	:					
			:			
·						

Examiner Signature	arstin	Dunger	Date Considered	09/29/2005
	0			

<sup>\*</sup>EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Burden Hour Statement: This form is estimated to take 2.0 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

<sup>&</sup>lt;sup>1</sup> Unique citation designation number. <sup>2</sup> Applicant is to place a check mark here if English language Translation is attached.

TOS(01/05/2005)(01)

PTO/SB/08a (08-03) Approved for use through 07/31/2006. OMB 0651-0031

U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no. sons are required to respond to a collection of info unless it contains a valid OMB control number.

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

of Sheet

Complete if Known			
Application Number	10/005,105		
Filing Date	December 3, 2001		
First Named Inventor	Paul C. Kocher		
Group Art Unit	2132		
Examiner Name	not yet known Justin T. Oarrow		
Attorney Docket Number	44424162-8721		

	U.S. PATENT DOCUMENTS $C(a_{s})$ $(a_{s})$							
Examiner Initials*	Cite No.1	Document Number Number-Kind Code <sup>2 (# known)</sup>	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear			
10		4,211,919 /	07/08/1980	Ugon	235/487			
7,0								
		· · · · · · · · · · · · · · · · · · ·						
			<u> </u>					
			·		·			
			1					

	FOREIGN PATENT DOCUMENTS							
Examiner	Cite No.1	Foreign Patent Number  Country Code <sup>3</sup> Number <sup>4</sup> Kind Code <sup>5</sup> (# known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	Te		

Examiner		Date	D 1/2 a 1/2
Signature	Justin Danon	Considered	0 \$129/2005

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. Applicant's unque citation designation number (optional). 2 See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. 3 Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). 4 For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. 5 Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file ( and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

IOS(12/27/2004) COM (12/2/2004)

PTO/SB/08a (08-03)

Approved for use through 07/31/2006. OMB 0651-0031

U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of info unless it contains a valid OMB control number.

RADE Trute for form 1449A/PTO

Sheet

## INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Complete if Known			
Application Number 10/005,105			
Filing Date December 3, 2001			
First Named Inventor	Paul C. Kocher		
Group Art Unit	2132		
Examiner Name	not yet known Juntin T. Damus		
Attorney Docket Number	44424162-8721		

	U.S. PATENT DOCUMENTS ( Lass / Cabolass							
Examiner Initials*	Cite No.1	Document Number  Number-Kind Code <sup>2 (f known)</sup>	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear			
go.		5,944,833 A	08/31/1999	Ugon	713/400			
			-					

	FOREIGN PATENT DOCUMENTS C 6051/5 45 c 641						
Examiner	Cite No.1	Foreign Patent Number	Publication Date	Name of Patentee or	Pages, Columns, Lines, Where Relevant Passages or	Te	
Initials*		Country Code <sup>3</sup> Number <sup>4</sup> Kind Code <sup>5</sup> (if known)	MM-DD-YYYY A	Applicant of Cited Document	Relevant Figures Appear		
NO		EP0826169B1	12/9/1997	Ugon	GO6F 1/04		
ADD.		EP1064752B1	23/09/1999	Salle	HOYL 9/06		
m		EP1204948B1	1/2/2001	Leydier	GOGK 19/073		

Examiner		Date	. 1 1
Signature	Matin amor	Considered	09/29/2005

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. ¹ Applicant's unque citation designation number (optional). ² See Kinds Codes of USPTO Patent Documents at <a href="https://www.uspto.gov">www.uspto.gov</a> or MPEP 901.04. ³ Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). ⁴For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁵ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁶ Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file ( and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

EDSC([[0P|2004)(0m 11/03/2004

PTO/SB/08a (08-03)

Approved for use through 07/31/2006. OMB 0651-0031

U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE binder the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of info unless it contains a valid OMB control number.

Substitute for form 1449A/PTO INFORMATION DISCLOSURE				Complete if Known		
				Application Number	10/005,105	
				Filing Date	December 3, 2001	
STA	STATEMENT BY APPLICANT			First Named Inventor	Paul C. Kocher	
				Group Art Unit	2132	
(use as many sheets as necessary)			as necessary)	Examiner Name	not yet known Juntin T. Damuw	
Sheet	1	of	2	Attorney Docket Number	44424162-8721	

		U	.S. PATENT DO	CUMENTS	(613/Sabely)
Examiner Initials*	Cite No.1	Document Number Number-Kind Code <sup>2 (# known)</sup>	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
AO		* 4,107,458 A	01/08/1978	Constant	178/22
000		*4,139,839 A	01/02/1979	Fletcher et al.	340/34700
180		* 4,569,052 A	04/02/1986	Cohn et al.	77//38
a	•	*4,605,921 A	08/01/1998	Riddle et al.	340/347 DO
10		*5,144,667 A	09/01/1992	Pogue et al.	300/45
N		* 5,159,632 /4	10/27/1992	Crandall	300/28
00		* 5,511,123 A	04/23/1996	Adams	380/29
10		* 5,551,013 A	08/27/1996	Beausoleil et al.	395/500
100		*5,559,890 A	09/09/1996	Obermeire et al.	S80 (4P
00		* 5,664,017 A	09/02/1997	Gressel et al.	380/30
00		* 5,710,834 A	01/01/1998	Rhoads	3P2/2J2
20		* 5,892,829 A	04/06/1999	Aiello et al.	3 PO /25
00		* 5,982,900 A	11/09/1999	Ebihara et al.	JP0/30
<del>- %</del>					

	FOREIGN PATENT DOCUMENTS							
Examiner Initials*	Cite No.1	Foreign Patent Number  Country Code* Number* Kind Code* (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	Te		
D		EP 0 660 562 A2	06/28/1995	General Instrument Corporation of Delaware	HO4L 9/00			

Examiner		Date 0.0/2.0/2.00	
Signature	Justin Janon	Considered 09/29/2007	

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. \ Applicant's unque citation designation number (optional). \ 2 See Kinds Codes of USPTO Patent Documents at <a href="https://www.uspto.gov">www.uspto.gov</a> or MPEP 901.04. \ 3 Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). \ 4 For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. \ 5 Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. \ 4 Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Approved for use through 10/31/2002. OMB 0651-0031

U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE Under the Paperwork Reduction Act of 1995 no persons are required to respond to a collection of info unless it contains a valid OMB control no.

Substitute for form 1449B/PTO 10 0 8 2003				Comple	ete if Known
				Application Number	10/005,105
				Filing Date	December 3, 2001
STATEMENT BY APPLICANT			PLICANT	First Named Inventor	Paul C. Kocher
				Group Art Unit	2132
	(use as many	sheel	s as necessary)	Examiner Name	not yet known Jurta T. Par
Sheet	2	of	2	Attorney Docket Number	44424162-8721

		OTHER ITEMS - NON PATENT LITERATURE DOCUMENTS	•
Examiner Initials*	Cite No.1	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T <sup>2</sup>
M		LACY, J. et al., "CryptoLib Version 1.1", File Bigpow.c from CryptoLib, United States, November 1999.	
no		"File NN.C from RSAFEF", RSA Laboratories, a division of RSA Data Security, Inc., United States, 1991.	
W		WAYNER, P., "Code Breaker Crack Smart Cards, Digital Safe", New York Times, United States, 06/22/98, on the World Wide Web at: http://www.nytimes.com/library/tech/98/06/biztech/articles/22card.html	
<i>0</i> 1			
······································		·	

Examiner		Date	0 / . /
Signature Our	tin Own	Considered	09/21/2005
1/1			

<sup>\*</sup>EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Burden Hour Statement: This form is estimated to take 2.0 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trudemark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

<sup>&</sup>lt;sup>1</sup> Unique citation designation number. <sup>2</sup> Applicant is to place a check mark here if English language Translation is attached.

JOS (09/24/2004) (om 09/22/2004

PTO/SB/08a (08-03)

Approved for use through 07/31/2006. OMB 0651-0031

U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE US DEPAR

Substitute for form 1449A/PTO Complete if Known 10/005,105 **Application Number** INFORMATION DISCLOSURE December 3, 2001 Filing Date STATEMENT BY APPLICANT Paul C. Kocher **First Named Inventor** 2132 **Group Art Unit** not yet known (use as many sheets as necessary) **Examiner Name** 44424162-8721 Scrinology Center 2 of Sheet Attorney Docket Number

	U.S. PATENT DOCUMENTS ( Loss / success									
Examiner Initials*	Cite No.1	Document Number  Number-Kind Code <sup>2 (# known)</sup>	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages Columns Lines, Where Relevant Rassages or Relevant Figures Appear					
an	AA	US-4,203,166 A	05/13/1980	Ehrsam et al.	375/2					
90	AB	US-4,214,126 A	07/22/1980	Wipff	179/1.5M					
20	AC	US-4,243,890 A	01/06/1981	Miller et al.	250/551					
m	AD	US-5,241,598 A	08/31/1993	Raith	300/21					
m	AE	US-5,297,201 A	03/22/1994	Dunlavy	3 80/6					
100	AF	US-5,341,423 A	08/23/1994	Nossen	380/6					
<i>"</i>	AG	US-5,369,706 A	11/29/1994	Latka	320/23					
M	AH	US-5,412,379 A	05/02/1995	Waraska et al.	340/025.72					
ha	Al	US-5,420,925 A	05/30/1995	Michaels	380/23					
100	AJ	US-5,544,086 A	08/06/1996	Davis et al.	364/408					
00	AK	US-5,552,776 A	09/03/1996	Wade et al.	340/P25,31					
- th	AL	US-5,559,887 A	09/24/1996	Davis et al.	300/24					
8	AM	US-5,600,324 A	02/04/1997	Reed et al.	3411,176					
7/1	AN	US-5,633,930 A	05/27/1997	Davis et al.	3POLX					
10	AO	US-5,733,047 A	03/31/1998	Furuta et al.	384143					
70	AP	US-5,761,306 A	06/02/1998	Lewis	34)/22					

	FOREIG	N PATENT DOC	UMENTS	(lass/subclass		
Cite No.1	Foreign Patent Number  Country Code <sup>2</sup> Number <sup>4</sup> Kind Code <sup>2</sup> (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	Te.	
AQ	EP 0 529 261 A2	03/03/1993	IBM Corp.	HO4L 9/08		
	EP 0 582 395 A2	02/09/1994	Digital Equipment Corp.	HO4L 29/06		
	Cite No.1  AQ  AR	Cite No.¹ Foreign Patent Number  Country Code³ Number⁴ Kind Code⁵ (if known)  AQ EP 0 529 261 A2	Cite No.¹         Foreign Patent Number Country Code³ Number⁴ Kind Code⁵ (if known)         Publication Date MM-DD-YYYY           AQ         EP 0 529 261 A2         03/03/1993	Country Code <sup>3</sup> Number <sup>4</sup> Kind Code <sup>5</sup> (if known) MM-DD-YYYY Applicant of Cited Document  AQ EP 0 529 261 A2 03/03/1993 IBM Corp.	Cite No.¹  Foreign Patent Number  Country Code³ Number⁴ Kind Code⁵ (if known)  AQ  EP 0 529 261 A2  Publication Date MM-DD-YYYY  Applicant of Cited Document  Name of Patentee or Applicant of Cited Document  Relevant Figures Appear  14 0 4 6 9 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	

Examiner		Date	09/29/2000
Signature	antin Rummy	Considered	0712112005
Y			_

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. ¹ Applicant's unque citation designation number (optional). ² See Kinds Codes of USPTO Patent Documents at <a href="https://www.uspto.gov">www.uspto.gov</a> or MPEP 901.04. ³ Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). ⁴For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁵ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Ĵ U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE · Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of info unless it contains a valid OMB control number. Complete if Known Substitute for form 1449A/PTO 10/005.105 **Application Number** December 3, 2001 INFORMATION DISCLOSURE Filing Date STATEMENT BY APPLICANT Paul C. Kocher **First Named Inventor** 2132 **Group Art Unit** Not yet know JunSEP (use as many sheets as necessary) **Examiner Name** 44424162-872 Sheet 2 Attorney Docket Number **U.S. PATENT DOCUMENTS** (las Pages, Columns, Lines **Document Number** Name of Patentee or **Publication Date** Examiner Cite Where Relevant Passages or Applicant of Cited Document MM-DD-YYYY Initials\* Number-Kind Code<sup>2 (# known)</sup> No. Relevant Figures Appear 07/07/1998 US-5,778,065 A Hauser, et al. RO /2/ 380128 Ab. 08/18/1998 Markham, Thomas R. US-5,796,836 A US-5,995,629 A 11/30/1999 Reiner WA THAT

		FOREIG	N PATENT DOC	UMENTS		
Examiner Initials*	Cite No.1	Foreign Patent Number  Country Code <sup>3</sup> Number Kind Code <sup>5</sup> (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	le
	-:-					
Examir Signat		Justin Danger		Date Considered	09/29/2005	

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. Applicant's unque citation designation number (optional). See Kinds Codes of USPTO Patent Documents at <a href="https://www.uspto.gov">www.uspto.gov</a> or MPEP 901.04. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. 5 Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file ( and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Please type a plus sign (+) inside this box TM +

Approved for use through 10/31/2002. OMB 0651-0031

U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of info unless it contains a valid OMB control no.

Substitute for form 1449B/PTO	Comple	ete if Known
	Application Number	10/005,105
INFORMATION DISCLOSURE	Filing Date	December 3, 2001
STATEMENT BY APPLICANT	First Named Inventor	Paul C. Kocher
h g	Group Art Unit	2132
(use as many sheets as necessary)	Examiner Name	not yet known Justin Tom
Speet 3 of 3	Attorney Docket Number	44424162-8721

		OTHER ITEMS - NON PATENT LITERATURE DOCUMENTS	
Examiner Initials*	CiteN o.¹	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T <sup>2</sup>
	AV	American National Standards for Financial Services, secretariat - American	
	1	Bankers Association (ANS/ABA x9.24-1997), "Financial Services Key	
1		Management," approved April 6, 1992, American National Standards	
- AI	<del> </del>	Institute; pgs. 1-71	+-
M	AW	JUENEMAN, Robert R., "Analysis of Certain Aspects of Output Feedback Mode", Satellite Business Systems, 1998; pgs. 99-127	
— (J.)	AX	BAUER, Friedrich L., "Cryptology - Methods and Maxims", Technical	Т
W		University Munich, 1998; pgs. 31-48	
(9)-	AY	CONNOR, Doug (Technical Editor), "Cryptographic Techniques - Secure	-
H		Your Wireless Designs", 01/18/96; pgs. 57-68	
<del>//-</del>	AZ	HORNAUER et al., "Markov Ciphers and Alternating Groups," Eurocrypt	
M		91, 1991; pgs. 453-460	-
1	BA	KOBLITZ, "A Course in Number Theory and Cryptography" 2e, 1994,	
10		Chapter III; pgs. 53-77	
	BB	LAI et al., "Markov Ciphers and Differential Cryptanalysis," Eurocrypt 91,	
RO		1991; pgs. 17-38	
	BC	HACHEZ et. al. "Timing Attack: What Can Be Achieved By A Powerful	
W		Adversary?" 1999	
(//	BD	KOCHER, Paul C., "Cryptanalysis of Diffie-Hellman, RSA, DSS, and	
RO		Other Systems Using Timing Attacks," Report 7 December 1995; pgs. 1-6	
	BE	KALISKI, Burt, "Timing Attacks on Cryptosystem," RSA Laboratories,	
W		Bulletin, Number 2, January 23, 1996	

Examiner Signature Owstin Jungar	Date Considered 09/29/2005	

<sup>\*</sup>EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Burden Hour Statement: This form is estimated to take 2.0 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

<sup>&</sup>lt;sup>1</sup> Unique citation designation number. <sup>2</sup> Applicant is to place a check mark here if English language Translation is attached.

	•			028420-0012CI	P	10/	005,105	
NE P	RMATION DISCLOSURE  BUS several sheets if necess			P. Kocher et al.			-	
6	ME &	•		FILING December 3, 20		ROUP 2	132	
C 144.		U.S	S. PATENT	DOCUMENTS	<u></u> L_		-03-611-0	
	ADEMATOCUMENT NUMBER	\ DATE		NAME	CLASS	SUBCLASS	FILING DAT	_
<i>a</i> O	4,200,770 A	4/1980	Hellmaı	et al.	178	22	T .	6/1977
gs	4,405,829 A	9/1983	Rivest e	t al.	178	22.1	12/1	(4/1977
22	4,759,063	7/1988	Chaum		380	30	08/2	2/1983
M	4,799,258 A	1/1989	Davies		380	21	02/0	7/1985
go	4,905,176 A	2/1990	Schulz		364	717	10/28	11988
90	<b>4,908,038</b> A	3/1990	Matsum	nura et al.	902	5	10/27	1/1888
go.	5,136,646 A	8/1992	Haber e	t al.	380	49	03/0	8/1981
D	5,297,207 <sub>A</sub>		Degele		380	46	05/24/1993	
go.			1995 Yoshida		235	487	02/18/1992	
go	O 5,404,402 A		4/1995 Sprunk		380	4	12/2/1993	
ap)	5,539,827 A		07/1996 Liu		380	37	04/05/1995	
V-		FORE	IGN PATE	NT DOCUMENTS				
	DOCUMENT NUMBER	DATE		COUNTRY	CLASS	SUBCLASS	TRANS YES	LATION
		,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,						
						ļ		
<u> </u>	OTHER DOCUME	NTS (Includin	g Author,	Title, Date, Pertinent F	Pages, Etc.)	I	L	
	"Security Requirements 140-1, U.S. Department	for Cryptograph of Commerce, Na	ic Module itional Inst	s," Federal Information Prittute of Standards and Tec	rocessing Star	idards Publica	tion (FIPS	PUB)
$  n_0  $					<u></u> ,			
W	RSA Data Security, RSA created 1991, pp. 1-2.	REF Cryptogra	phic Toolk	it Source Code, File R_RA	NDOM.C, av	ailable from f	tp://ftp.rsa	.com,
go								
EXAMINER	<i>t</i>			DATE CONSIDERED	1/29/20	ur		·
*EXAMINER: Initia	to: Allows  al if reference considered, whether de copy of this form with next com						onformance	and not

TOC(01/1/2000) (0M (1/16/200)

Form PTO-A820 (also form PTO-1449) P09C/REV03

Patent and Trademark Office \* U.S. DEPARTMENT OF COMMERCE

ابر	•				028420-0012	CIP	3ERIAL NO. 10/	005,105	
	y the development of the second of the secon				P. Kocher et al.				
					FILING December 3, 2001		GROUP 2132 -Unassigned-		
	(	141 31 Due (c)		DATENT		2001	044	essigned.	
	1		U.S	AIENI	DOCUMENTS				
*EXAMINER INITIAL	-	TRADEN NUMBER	DATE		NAME	CLASS	SUBCLASS	FILING DATI	
<i>g</i>		5,546,463 A	8/1996	Caputo	et al.	380	25	07/1	2/1994
ŊΩ		5,663,896 A	9/1997	Aucsmi	th	395	187.01	09/2	
M		5,664,017 A	9/1997	Gressel	et al.	380	30	120	OP/1905
(A)		5,727,063 A	3/1998	Aiello e	t al.	380	46	11/2	27/12/5
20		5,778,074 A	7/1998	Garcke	n et al.	380	37	06/2	8/1196
00		5,812,669	9/1998	Jenkins	et al.	380	25	07/19	9/1895
DO		<b>5,835,599</b> A	11/1998	Buer		380	29	04/1	5/1396
JP)		5,838,795	11/1998	Mittenthal		380	28	07/0	57/1887
B	5,848,159		12/1998	Collins et al.		380	30	01/1	6/1497
10			11/1999	Shamir		380	30	05/12/897	
m		6,041,122 A	03/2000 Gra		Graunke et al.		21	02/2-	
			FORE	IGN PATE	ATENT DOCUMENTS				
		DOCUMENT NUMBER	DATE		COUNTRY	CLASS	SUBCLASS	TRANS	LATION NO
			,		· ·				
							:		
		**************************************					<u>-</u>		
					<u> </u>				
	11_	OTHER DOCUME	NTS (Includin	l a Author	Title, Date, Pertinen	t Pages Ftc	<u> </u>	I	L
		M. Bellare et al., "Incre Crypto 94 Proceedings (					<del>-</del>	ances in Cr	yptology -
0.0		or y pro > 4 1 recembes (	~F1 111861 . 4 61 148	, .,, ., pp.					
-1//	+	Paul C. Kocher, "Timin Advances in Cryptology	g Attacks on Imp	erlin, Sprin	ons of Diffie-Hellman, R.	SA, DSS, and C	Other Systems,'	'in: Kobli	tz, N.,
00		3,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	2.000000	, op. 10	.0				
EXAMINE	R		· · · · · · · · · · · · · · · · · · ·		DATE CONSIDERED	0./ /			
	Just	- Janon				09/29/	2005		
		if reference considered, whethe copy of this form with next con			ance with MPEP 609; Dra	w line through o	itation if not in c	onformance	and not

٠				ATTY DOCKET NO. 028420-00120		SERIAL NO. 10/	005,105	
	INFORMATION DISCLOSURE			P. Kocher et al.	<u> </u>			
	(Use several shorts in access	a.y,		FILING		GROUP )	13.2	
		<u> </u>		December 3, 2		~ <del>Û</del> n:	132 assigned	
	JAN 3 1 2002	U.	S. PATENT	DOCUMENTS				
*EXAMINER INITIAL	DOCUMENT NUMBER	DATE	<u></u>	NAME	CLASS	SUBCLASS	FILING DAT	_
ΔΩ	6,041,412 A	3/2000	Timson	, et al.	713	200	11 (14	11997
M	6,049,613 A	4/2000	Jakobss	on	380	47	01/13	11998
N	<b>6,064,724</b> A	5/2000	Kelly		379	92.04	11/22	11996
m	6,064,740 A	5/2000	Curiger	et al.	380	265	11/12	/1997
B	6,069,954 A	5/2000	Moreau	<u> </u>	380	28	05/09	1197
7						_	<u> </u>	
							:	
_								
		FORE	IGN PATE	NT DOCUMENTS				
	DOCUMENT NUMBER	DATE		COUNTRY	CLASS	SUBCLASS	TRANSI YES	ATION NO
				_3333333				
	OTHER DOCUME			, Title, Date, Pertinent		·		
	Schneier, Bruce, Applied Inc. 10/18/95, pp. 34-41,	d Cryptography, 390-392 and 480	Second Ed 0-481.	lition: Protocols, Algorit	hms, and Sou	rce Code in C,"	John Wile	y & Sons,
	Krawczyk, H., et al., "H Comments RFC 2104, F	MAC: Keyed-H ebruary 1997, p	lashing for p. 1-11.	Message Authentication,	" Network W	orking Group	Request for	
an)								
EXAMINER	North Danger		,	DATE CONSIDERED	19/29/2	BUT		
*EXAMINE	R: Initial if reference considered, whether	r or not citation is	in conform			<del></del>	onformance	and not
	. Include copy of this form with next con							

Form PTO-A820 (also form PTO-1449)

Copyright 1994-97 LegatStar

P09C/REV03

Patent and Trademark Office \* U.S. DEPARTMENT OF COMMERCE

information disclosure citation (Use several sheets if necessary)		Docket Number (Optional)	Application Number	
		028420-0012CIP	10/005,105	
		Applicant(s)		
		P. Kocher et al.		
		Filing Date December 3, 2001	Group Art Unit 2 132 Unassigned	
		December 3, 2001	Chancigned	
*EXAMINER INITIAL	OTHER DOCUMENTS (Including Author, 7	itle, Date, Pertinent Pages, Etc.)		
OIP	Ryan, J. "Blinds for Thermodynamic Cipher Attacks," unpublished material on the World Wide Web at http://www.cybertrace.com/thrmatak.html, March 1996, pp. 1-7.			
/0		Anttp://www.cybertrace.com/inrmatak.ntmi, waren 1996, pp. 1-7.		
1 mm 21	and 3			
MAN 31	Data Encryption Standard." Federal Information	Data Encryption Standard," Federal Information Processing Standards Publication (FIPS PUB) 46-2, U.S. Department of		
7	Commerce, National Institute of Standards and T	Commerce, National Institute of Standards and Technology, December 30, 1993, pp. 1-21.		
TRADE	MARKE			
(f) =				
	Biham, E., et al., "Differential Fault Analysis of S Cryptology-CRYPTO '97 (Berlin, Springer, 1997	ecret Key Cryptosystems," in: Kalisk ), 17th Annual International Cryptolo	d, B., Advances in gy Conference, August 17-21, 1997, pp.	
	513-525.	513-525.		
20_				
<i>y</i> ,	Based on "Karn/Hoey/Outerbridge" implementation (KHODES): "File DESC.C from RSAREF - Data Encryption Standard routines for RSAREF."			
$\mathcal{M}$				
<i>y.</i>	Alfred J. Menezes et al., "Handbook of Applied Cryptography" (CRC Press, 1996), pages including 285-298, 312-319,			
	452-462, 475, 515-524.			
$\alpha$				
	Bank Technology News. Cries of Wolf Over Sma	rt Card Security? Faulkner & Gray.	Inc. 01 November 1996.	
	ball technology with a cried of world over bline	. Cara Searniy. Tannae. a G.ay,		
20		,		
-/ <i>J</i>				
			į	
EXAMINER		DATE CONSIDERED		
$\Omega$	notin Domer	09/29/2005		
7720.001				
EXAMINER: Initial if citation considered, whether or not citation is in conformance with MPEP Section 609; Draw line through citation if not in conformance and				

P098/REV04

not considered. Include copy of this form with next communication to applicant.